信息安全课程实验二

1. **实验目的**

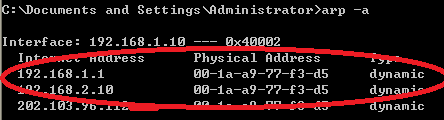
学习虚拟机安装，版本控制Git软件、收发包、抓包软件使用及初步具备协议分析能力；

1. **实验工具**

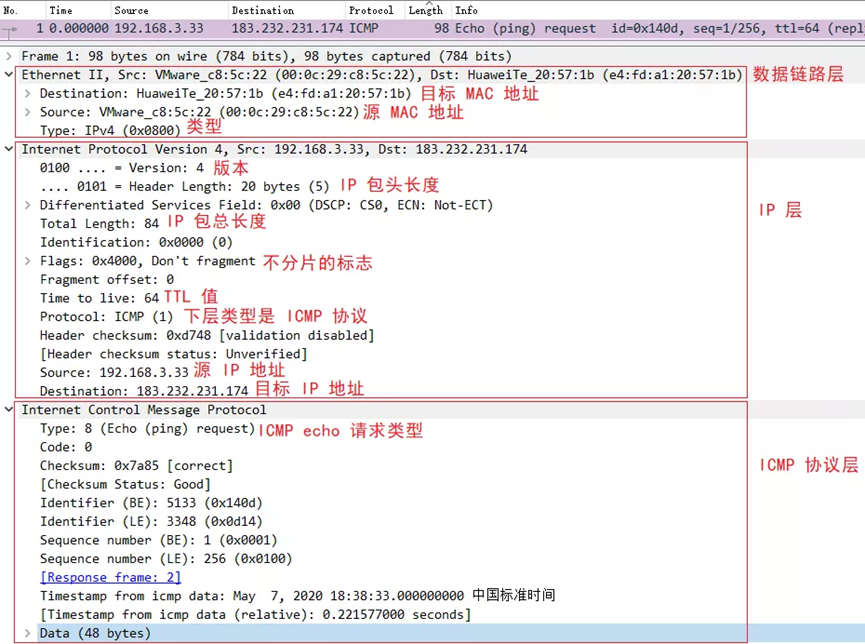
Centos6以上系统，GitHub，科来数据包生成器/科来数据包播放器软件（pktbuilder\_x64/pktplayer\_x64），Wireshark

1. **实验内容**
2. 采用科来数据包生成器生成三种ARP协议数据包（请求、应答、免费(Gratuitous ARP)三种形式的ARP包；

B、采用科来数据包播放器软件将三种伪造数据包向攻击目标机发送，检验三种形式的ARP包是否具备断网攻击能力（采用arp命令查看攻击前后的目标机ARP缓存表是否发生变化并截图说明）



C、整个攻击过程采用Wireshark进行抓包并参考如下图对三种ARP协议进行协议分析和标注，同时对应攻击数据包导出以pcap包格式保存；



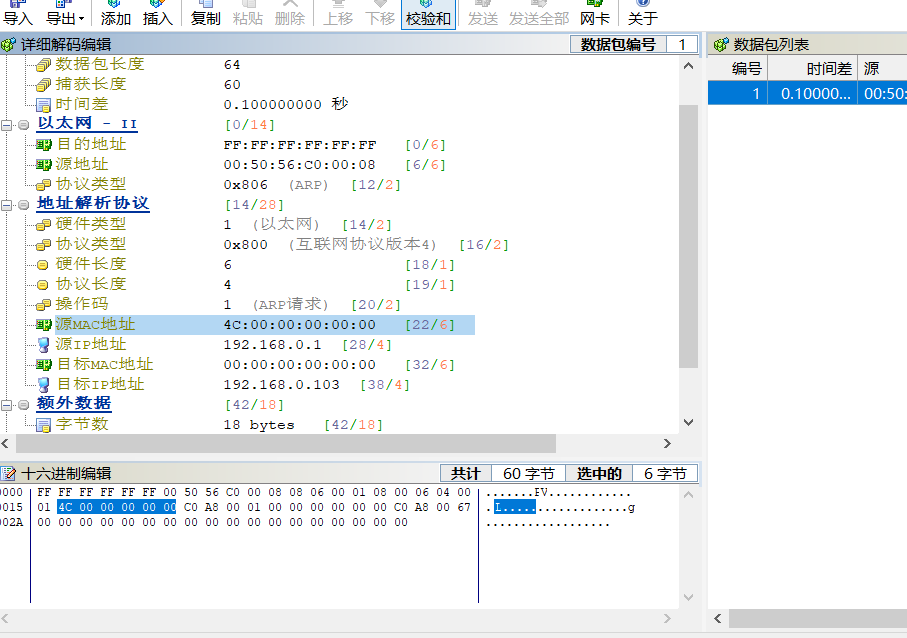
D、针对ARP攻击，如何进行防护，请提出自己的意见和建议。

1. **实验报告要求**
2. 对实验过程进行截图，并配合文字详述以上实验内容；
3. 对实验报告中引用的互联网资料，需要以参考文献形式加以引用标注
4. **实验报告上交截止时间**

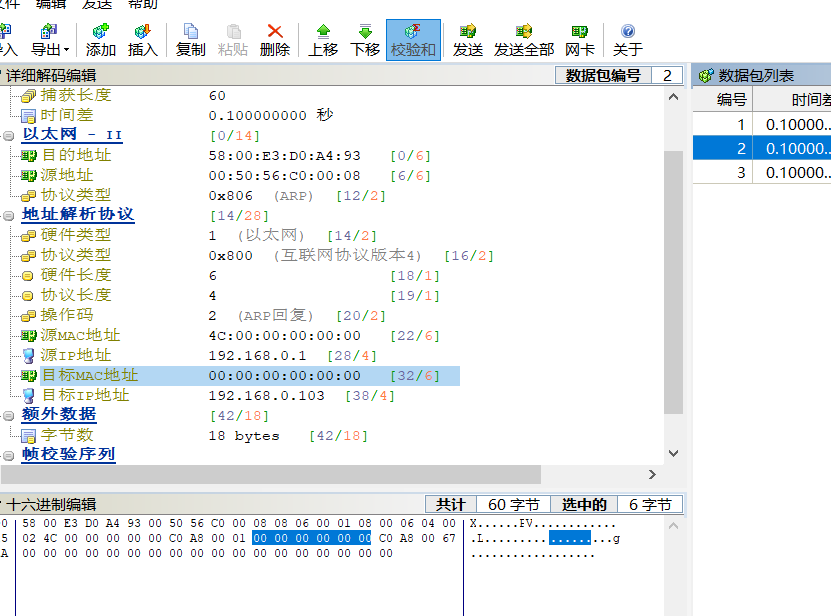
作业内容包括：三种ARP协议的PCAP数据包文件（共三个文件），实验报告一份，将这些内容上传github进行版本控制。[2020年5月11日18点前将作业的github下载链接发zhxhz@163.com](mailto:2020年5月11日18点前将作业的github下载链接发zhxhz@163.com)邮箱。

1. 采用科来数据包生成器生成三种ARP协议数据包（请求、应答、免费(Gratuitous ARP)三种形式的ARP包；

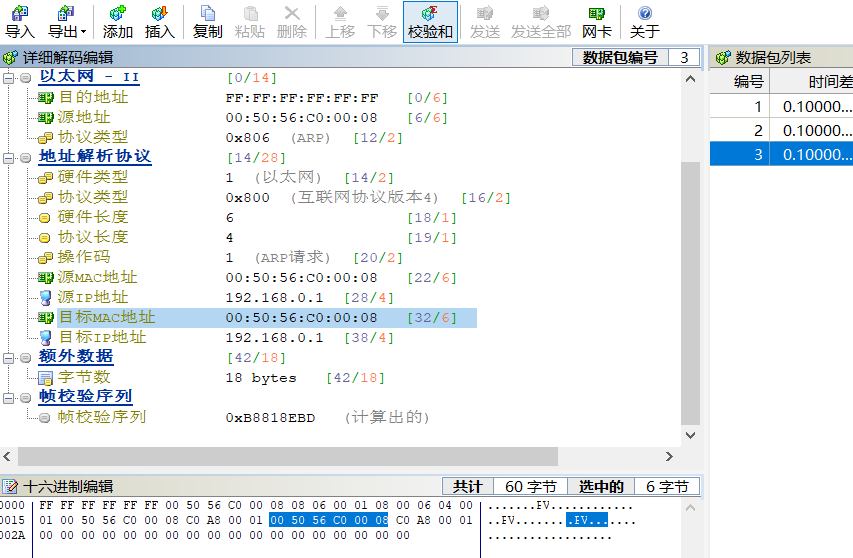
1.生成请求包



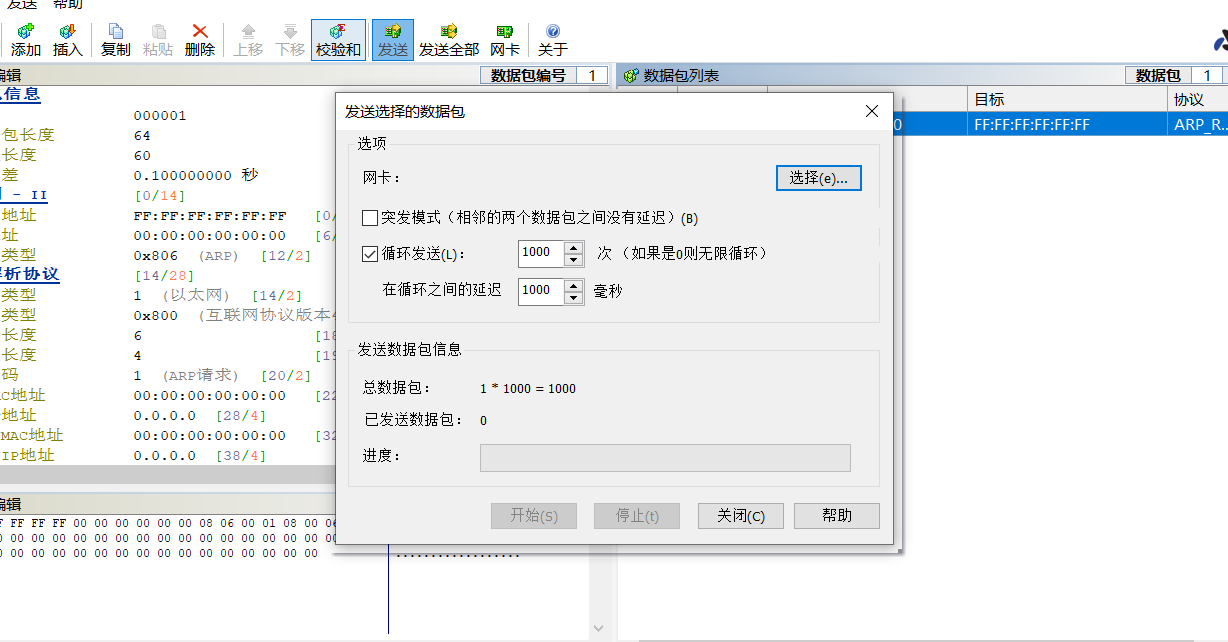
生成应答包



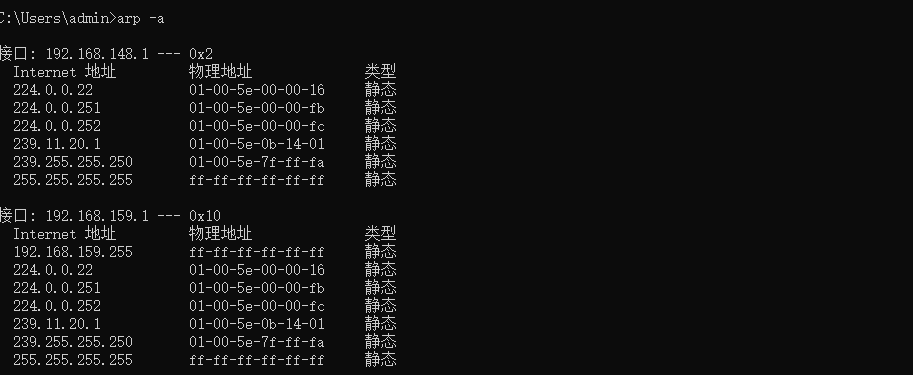
生成免费包



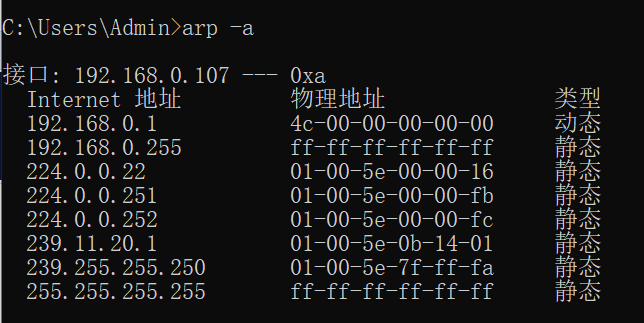
1. 设置发送循环次数



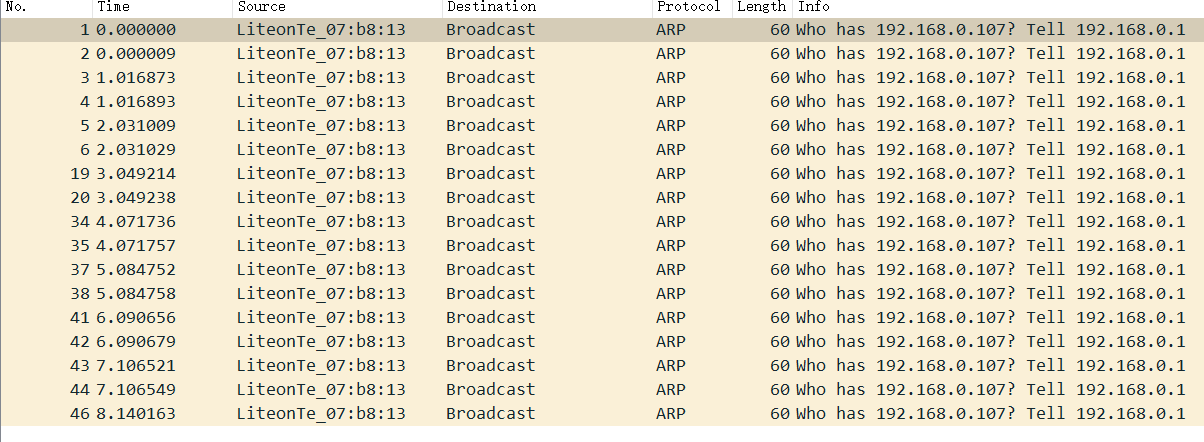
1. 利用arp -a 查看发送之前ARP缓存表



1. 发送之后



利用抓包工具进行抓包



被攻击者已经断网

总结：

1.Windows10读取不到网卡，不能发送ARP包

2.需要提前知道被攻击者的mac地址和IP地址